USAPA Sunset Provisions Could Leave Congress in the Dark

The USA Patriot Act (USAPA) represents a sweeping increase in the power of both domestic law enforcement and international intelligence agencies. With almost no debate and a suspension of the normal review processes, Congress opened the door for a much more in surveillance of both American citizens and immigrants.

During the abbreviated legislative process, several members of Congress expressed concern about its breadth, about the lack of debate and the suspension of normal Congressional processes. As a result of these concerns, USAPA §224 was added. This section, appropriately titled "Sunset," set an expiration date of December 31, 2005 for several of the surveillance provisions of the new law. The Sunset provision was intended to give Congress and the public the chance to evaluate how law enforcement exercised some of its broad new powers and to decide whether the serious reduction of American privacy and civil liberties enacted by USAPA was worthwhile.

Yet without a vigilant public and diligent exercise of power by Congress, there will be no objective factual basis on which to evaluate the impact of USAPA. This is because little or no reporting is currently required by intelligence agencies or law enforcement about how they use these new powers.

EFF urges Congress members, especially those of the Intelligence and Judiciary Committees, to exercise their plenary powers to hold oversight hearings and require ongoing comprehensive reports about how these new powers are being used and that, whenever possible, the information contained in those reports be provided to the public. Such hearings should begin immediately, since the powers granted by USAPA are already being used. They should continue periodically through 2005 and, if necessary, beyond that date.

I. FISA

The Foreign Intelligence Surveillance Act, passed in 1978, allows a secret court to authorize surveillance of foreign agents, including US persons, most often by the Department of Justice. The FISA statute does not allow public release of any substantive information about the requests it reviews. In FISA's history, the secret court appears to have only refused a single request for surveillance out of over 10,000 requests. In the case of pen/trap requests (which include web surfing habits and all "non-content" information contained in e-mails) and subpoenas of stored information, the FISA statute does not require the agency conducting the surveillance to report back to the FISA court how the FISA warrants for were actually used. That means that the issuing court does not know whether the warrant provided any useful information or whether it was misused.

The only information publicly released about the FISA process is the number of requests made and the number granted. The statute does provide for a more thorough, but secret, report to the Permanent Select Committee on Intelligence in the House and the Select Committee on Intelligence in the Senate, but it does not provide for any additional information to be given to Congress as a whole. Although this lack of public information was troubling prior to the passage of the USAPA, it will now leave Congress with little basis upon which to evaluate the broad new powers it has granted when they come up for renewal in 2005. If the entire Congress is to decide whether the increased authority given under USAPA is warranted, reporting on the use of such authority should not be limited to the Intelligence Committees.

A. USAPA Expands the Scope of FISA Surveillance

The USAPA dramatically expands governmental power regarding wiretaps, pen/trap orders and subpoenas under the Foreign Intelligence Surveillance Act (FISA) and in large measure tears down the wall between foreign intelligence and domestic law enforcement erected after the revelations, in the 1970s, that the FBI had opened files on over one million Americans and actively investigated over 500,000 without a single conviction of illegal activity.[1] Yet despite their history and the grave risk they pose to civil liberties, when these provisions come up for renewal in 2005 Congress will have little information about how these new powers have been used unless it takes affirmative steps to subpoena the relevant information.

B. The Specific Provisions that Broaden the Scope of FISA Surveillance

Sec. 218: With the passage of USAPA, FISA can now be used in domestic criminal investigations. The Attorney General need only certify that foreign intelligence gathering is a "significant purpose" (§218), not "the purpose," when requesting FISA powers. However, since the "purpose" of FISA warrants is never reported, Congress will have no way to evaluate whether this expansion resulted in a greater number of arrests, prevented terrorism or was used mainly for criminal investigations.

Sec. 206: USAPA allows FISA warrants to be "roving," -- that is that a single warrant may be served on any provider of Internet or other communications service, regardless of whether that provider is named in the warrant. As with the other new FISA authorities, there is no way for Congress to evaluate whether this new power is being carefully used only to monitor targets, or whether it becomes a tool for broad fishing expeditions by foreign intelligence into the e-mail and other communications of innocent Americans.

---

[1] EFF's complete description of USAPA as it relates to online activities and surveillance is contained here. http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html.

Sec. 215: FISA warrants may now be used to access a much broader range of business records of US citizens than previously allowed, except investigations based solely on the basis of First Amendment activities. Again, outside of the intelligence committees, Congress will have no way to know how this broad authority was used, how many citizens had their records compelled by this law and whether and how that information was used in fighting terrorism. This provision expressly provides that a report shall be made semi-annually to Congress containing only the total number of requests made and the total number granted, denied or modified.

II. Wall Between Domestic Law Enforcement and Intelligence Agencies is Torn Down

Sec. 203: In addition to expressly allowing FISA surveillance for matters only "substantially" related to foreign intelligence, USAPA directly breaks down many of the barriers that had previously prevented sharing of foreign and domestic surveillance information. It also adds a new category of information that may be shared, called Foreign Intelligence Information. But there is no provision for the intelligence agencies or the domestic law enforcement to report to Congress about how much and what type of information sharing is actually done under this new law. Without this information, Congress will be unable to rationally decide whether the wall between domestic and international surveillance built after the scandals of the McCarthy and civil rights eras should remain torn down or be rebuilt.

III. Exceeding the Authority Granted on a Computer

Sec. 217. This section eliminates any judicial participation in wiretaps of those suspected of having exceeded the "authorization" granted to them on another's computers. Although the obvious application of this statute is those alleged to be computer "trespassers" the language of the statute is much broader and has been applied in the past to those sending unsolicited e-mail and low level computer intrusions such as those done for political protest.

Under the new provision, if a computer owner or operator consents, law enforcement can obtain both the content and non-content portions of all messages sent by someone suspected of exceeding their authority on a computer through the computer. The threshold for such broad authority is when law enforcement agent "has reasonable grounds to believe contents of communication will be relevant" to investigating computer trespass and when law enforcement does not acquire anyone else's communications. This provision is problematic both because it has no reasonable relationship to terrorism and because its broad application could result in unsupervised surveillance of Americans.

As with the other provisions noted above, however, neither the USAPA nor existing law require that law enforcement inform Congress or the public about how this new power is being used. And there is no need for Court authorization. Thus, when this provision comes up for renewal in 2005, unless Congress has used its plenary power to demand reporting, neither Congress nor the public will be able to decide whether this

provision has been applied narrowly or broadly, whether its legal contours (such as requiring that no other person's e-mail is acquired) are in fact being followed or, most importantly, whether this power has actually proved to be a useful tool in the fight against terrorism.

What Reporting Should Look Like

Congress has plenary powers that enable it to require detailed, comprehensive reporting by the domestic and international intelligence agencies about how they have used the powers recently granted to them by Congress. Although in the past, such powers have been mainly used by the House and Senate intelligence committees, nothing requires that reporting be limited to just these Congress members. In the extraordinary case of the USAPA, the renewal of these statutes will be before the entire Congress in 2005. Given this, members of Congress outside of those committees, especially those on the Judiciary Committees where the USAPA originated, should use their plenary power to require detailed reporting. Moreover, the American people should be allowed to see how these powers have been used, except where such information is specifically classified by the agencies.

These reports should include the following, at a minimum:

1. The type and scope of applications made.
2. The basis for the request, including
    a. what underlying crime was suspected,
    b. what is the basis for belief that the person has relevant information.
3. Who the warrant or order was served upon, including both those named and any others served as part of a "roving" wiretap.
4. The type and amount of information gathered, including the how many third parties were involved as senders to or from the target or the surveillance.
5. Whether the information was ultimately used in prosecution of terrorism or any other offenses or to further an investigation that later bore fruit.
6. How the information was shared and how shared information was ultimately used.
7. Categorizing the requests into those aimed at fighting terrorism and those aimed at domestic law enforcement.

Conclusion

The EFF remains deeply troubled that Congress has passed such sweeping reductions in the right of Americans to be free from overarching government surveillance. Yet having done so, it is imperative that Congress fulfill the promise of the Sunset provisions by requiring and, where possible, sharing with the American people basic information about how these broad new powers are being used.